(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
10 June 2004 (10.06.2004)

PCT

(10) International Publication Number
WO 2004/049153 A3

(51) International Patent Classification[7]: G06F 9/32

(21) International Application Number: PCT/IB2003/005155

(22) International Filing Date: 13 November 2003 (13.11.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
102 54 658.4 22 November 2002 (22.11.2002) DE

(71) Applicant *(for DE only)*: **PHILIPS INTELLECTUAL PROPERTY & STANDARDS GMBH** [DE/DE]; Steindamm 94, 20099 Hamburg (DE).

(71) Applicant *(for all designated States except DE, US)*: **KONINKLIJKE PHILIPS ELECTRONICS N.V.** [NL/NL]; Groenewoudseweg 1, NL-5621 BA Eindhoven (NL).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **MUELLER, Detlef** [DE/DE]; c/o Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

(74) Agent: **MEYER, Michael**; Philips Intellectual Property & Standards GmbH, Weisshausstr. 2, 52066 Aachen (DE).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report: 28 October 2004

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 2004/049153 A3

(54) Title: METHOD AND APPARATUS FOR PROCESSING CONDITIONAL BRANCH INSTRUCTIONS

(57) Abstract: In the programming of a microcontroller (100) carried out in at least one machine-dependent assembly language in which the assembler commands, with the exception of conditional program branches, are executable essentially independently of data,- in case of a fulfilled branch condition, for example, at least one fulfilled status flag, at least one program counter (10) is loadable with a new address and/or a new value, and- in case of an unfulfilled branch condition, for example, at least one unfulfilled status flag, the instruction is ended. To further develop said programming, together with a method for processing the programming of the microcontroller (100) carried out in at least one machine-dependent assembly language, in such a way that it is invisible from outside whether or not, in the case of a conditional program branch, said branch has actually taken place, it is proposed that, in the case of an unfulfilled branch condition, the program counter (10) is optionally re-loadable with its previous address and/or with its previous value, instead of ending the instruction.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 03/05155

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 690 370 A (SOFTCHIP ISRAEL LTD) 3 January 1996 (1996-01-03) page 8, line 41 - page 9, line 29; claim 9; figure 7	1-6,8-10
X	WO 00/05837 A (CERTICOM CORP ; VADEKAR ASHOK (CA); LAMBERT ROBERT J (CA)) 3 February 2000 (2000-02-03) page 2, line 25 - line 28 page 5, line 12 - page 6, line 13	1-6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 August 2004	20/08/2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Moraiti, M

INTERNATIONAL SEARCH REPORT

International Application No
PCT/IB 03/05155

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KOCHER P C ED - KOBLITZ N (ED) INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH: "TIMING ATTACKS ON IMPLEMENTATIONS OF DIFFIE-HELLMAN, RSA, DSS, AND OTHER SYSTEMS" ADVANCES IN CRYPTOLOGY - CRYPTO '96. 16TH. ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, AUG. 18 - 22, 1996. PROCEEDINGS, PROCEEDINGS OF THE ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE (CRYPTO), BERLIN, SPRINGER, DE, vol. CONF. 16, 18 August 1996 (1996-08-18), pages 104-113, XP000626590 ISBN: 3-540-61512-1	

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 03/05155

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0690370 A	03-01-1996	IL 110181 A	08-02-1998
		EP 0690370 A2	03-01-1996
		JP 8328848 A	13-12-1996
		US 5729766 A	17-03-1998
WO 0005837 A	03-02-2000	CA 2243761 A1	21-01-2000
		AU 4891799 A	14-02-2000
		WO 0005837 A1	03-02-2000
		EP 1097541 A1	09-05-2001
		JP 2002521724 T	16-07-2002
		US 2001033655 A1	25-10-2001